



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,645	01/24/2004	Ron Khormaei	100201951-1	9156
22879 7590 09/18/2007 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			EXAMINER KIM, JUNG W	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 09/18/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/764,645	Applicant(s) KHORMAEI ET AL.	
	Examiner Jung Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office action is in response to the amendment filed on 7/25/07.
2. Claims 1-25 are pending.

Response to Arguments

3. Applicant's arguments with respect to the prior art rejections have been fully considered but they are not persuasive.

4. On pg. 8-9 of the Remarks, applicant alleges that Tresser does not anticipate the amendment claims because Tresser only discloses employing a mathematical process that involves a portion of data set, whereas the claims require that a mathematical process involve the entire data set. (applicant points to the section of Tresser [col. 9:8-19] that discloses the processed signal is further cut into a plurality of pieces and then either compressed or signed) However, Tresser discloses that the data stream is "optionally" cut into a plurality of pieces. Hence, Tresser discloses an embodiment wherein the data stream is not divided into a plurality of pieces. In this particular embodiment, the signing step (col. 9:25-32) involves the entire data set. Therefore, Tresser discloses employing a mathematical process that involves the entire data set.

5. In response to applicant's argument that Tresser does not disclose that the halftone image is produced from the original image because Tresser discloses that a new image is first computed out of the original image by covering the original image with a grid of size H-by-V, and then averaging the grey levels on the little rectangles defined

by the grid, is not persuasive. The fact that Tresser discloses a halftone image is produce from a digital file that is representative of a document, anticipates this limitation of the claims. Applicant's argument appears to be attempting to define a difference in the claimed language of the instant invention and Tresser. However, the features upon which applicant relies (i.e., a halftoning image is produced directly from the original image with out any intervening transformations) are not recited in the rejected claim(s). Moreover, although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. On pgs. 11-12, applicant alleges the following:

However, after a thorough search of Tresser, the Applicants find no teaching or suggestion of both a sender computer and a receiver computer configured as claimed, nor do the Applicants find any teaching or suggestion of both a sender printer and a receiver printer configured as claimed. Rather Tresser discloses, at most, a single computer and a single printer.

7. Applicant's through examination of Tresser is noted. However, the Office's position is that Tresser expressly discloses a sender computer and printer (col. 8:36-40), and a receiver computer and printer (col. 10:31-35; fig. 6, reference no. 620, fig. 7, reference no. 739) Furthermore, contrary to applicant's allegations, Tresser discloses performing a predetermined mathematical process on the first plurality of discrete digital values to thereby generate a sender authentication key AND perform the predefined mathematical process on the second plurality of discrete digital values to thereby generate a receiver authentication key as outlined below in the rejections.

8. Finally, applicant's allegation that "Tresser teaches that it is preferable to not have a computer" (Remarks, pg. 12 4th full paragraph) because "Tresser teaches that it is preferable to provide a scanner with 'enough computing power to dispense of the computer,'" is an improper conclusion based on the disclosure of Tresser. Tresser never suggests "that it's preferable to not have a computer"; rather, Tresser discloses that the scanner have enough computing power to dispense of the computer attached to the scanner as illustrated in fig. 6. ("the scanner can be a hand-held device, which can also have enough computing power to dispense of the computer at 620," col. 10:1-3) Hence Tresser is actually suggesting that the scanner can be provided with enough computing power so that the scanner by itself is a fully operational computer. Hence, applicant's argument that "Tresser teaches that it is preferable to not have a computer" is without merit.

9. For these reasons, the claims remain rejected under the prior art of record.

Claim Rejections - 35 USC § 102

10. Claims 1-11 and 14-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Tresser et al. USPN 6,804,373 (hereinafter Tresser).

11. As per claims 1-6, Tresser discloses a method of generating an authentication key that can be used to authenticate an electronic document file representative of a document, comprising:

- a. providing the electronic document file as an initial digital file; (col. 8:56)

- b. applying a predetermined halftoning process to the digital file to generate a digital halftone file defined by a plurality of discrete digital values; (9:4-7 and lines 40-44)
 - c. performing a predetermined mathematical process involving each of the plurality of discrete digital values to thereby generate the authentication key; (9:7-32)
 - d. printing the digital halftone file to provide a tangible copy of the document containing a visible representation of the authentication key; (9:66-10:5)
 - e. displaying the digital halftone file on a user display to provide a visible copy of the document and the authentication key; (10:61-64)
 - f. wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm; (5:30-31 and lines 41-44)
 - g. wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm; (5:15-41; 9:4-7) and
 - h. wherein the predetermined mathematical process is a summation process. (6:6-25)
12. As per claims 7-11, Tresser discloses a method of authenticating an electronic document file representative of a document, comprising:
- i. receiving the electronic document file as an initial digital file; applying a predetermined halftoning process to the digital file to generate a digital halftone

file defined by a plurality of discrete digital values; performing a predetermined mathematical process involving each of the plurality of discrete digital values to generate an authentication key; and using the authentication key to authenticate the electronic document file; wherein using the authentication key to authenticate the electronic document file comprises: receiving a sender authentication key; and comparing the sender authentication key to the generated authentication key and, if the keys are the same, authenticity of the electronic document file is verified; (col. 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N'; embedded matrix M is necessarily transformed to compressed version of half tone N, whereby a match authenticates the document)

j. wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm; (5:30-31 and lines 41-44)

k. wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm; and (5:15-41; 9:4-7)

l. wherein the predetermined mathematical process is a summation process. (6:6-25)

13. As per claim 14, Tresser discloses a system to generate an authentication key to be used to authenticate an electronic document file representative of a document, comprising: a processor; and a computer readable memory device which is readable by

Art Unit: 2132

the processor (fig. 7 and related text), the computer readable memory device containing a series of computer executable steps configured to cause the processor to: retrieve a copy of the electronic document file as an initial digital file (col. 8:56-63); apply a predetermined halftoning process to the initial digital file to generate a digital halftone file defined by a plurality of discrete digital values (9:4-7 and lines 40-44); perform a predetermined mathematical process involving each of the plurality of discrete digital values to thereby generate the authentication key (9:17-19 and lines 25-32); and store a copy of the authentication key in the computer readable memory device. (fig. 3, reference no. 380; 10:53-54)

14. As per claim 15, Tresser further discloses wherein the processor and the computer readable memory device are resident within a document printing device. (col. 1:10-12; fig. 7, reference no. 739)

15. As per claim 16, Tresser further discloses wherein the series of computer executable steps are further configured to cause the processor to print a tangible copy of the halftone image file as the document, and to include the authentication key on the tangible copy of the halftone image file. (Col. 9:66-10:5)

16. As per claim 17, Tresser further discloses wherein the computer readable memory is configured to store, at least temporarily, a copy of the electronic document file as the initial digital document file. (fig. 3, reference no. 380; 10:53-54)

17. As per claim 18, Tresser discloses the system further comprising a user display, and wherein the series of computer executable steps are further configured to cause the processor to display, via the user display, the authentication key. (Col. 10:61-64)

Claim Rejections - 35 USC § 103

18. Claims 12 and 13 are rejected under 35 USC 103(a) as being unpatentable over Tresser in view of Linsker et al. USPN 5,598,473 (hereinafter Linsker).

19. As per claims 12 and 13, the rejections of claims 9 and 10 as being anticipated by Tresser are incorporated herein. Tresser does not disclose wherein the electronic document file is received from a sender via a network and wherein the sender authentication key is received via one of telephone or facsimile. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital document to create a second digest, wherein a match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the electronic document file of Tresser to be received from a sender via a network and wherein the sender authentication key is received via one of telephone or facsimile.

One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 12 and 13.

20. Claims 19, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tresser in view of Brundage et al. US Patent Application Publication No. 20040181671 (hereinafter Brundage).

21. As per claim 19, Tresser discloses a system for authenticating an electronic document file representative of a document, comprising: a processor; a computer readable memory device which is readable by the processor (fig. 7 and related text) and which is configured to receive the electronic document file as an initial digital file; and wherein: the computer readable memory device contains a series of computer executable steps configured to cause the processor to: store the initial digital file in the computer readable memory device; apply a predetermined halftoning process to the initial digital file to generate a digital halftone file defined by a plurality of discrete digital values; perform a predetermined mathematical process involving each of the plurality of discrete digital values to thereby generate the authentication key. (col. 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N';

embedded matrix M is transformed to compressed version of half tone N, a match authenticates the document)

22. Tresser does not disclose displaying a copy of the authentication key to a user via one of a printer or a user display. Brundage discloses a system for authenticating identification documents using a watermark, wherein an authenticator displays the watermark information to a user to allow an inspector or officer to visually compare the watermark information against information printed on the document. Paragraph 62. It would be obvious to one of ordinary skill in the art at the time the invention was made to display a copy of the authentication key to a user via one of a printer or a user display. One would be motivated to do so to enable a human to quantify the authenticity of the document as taught by Brundage, *ibid*. The aforementioned cover the limitations of claim 19.

23. As per claim 22, the rejection of claim 19 under 35 USC 103(a) as being unpatentable over 35 USC 103(a) is incorporated herein. In addition, Tresser discloses wherein the processor and the computer readable memory device are resident within a document printing device. (col. 1:10-12; fig. 7, reference no. 739)

24. As per claim 23, Tresser discloses an system to authenticate an electronic document file, comprising:

- m. a sender computer configured to provide the electronic document file in the form of a sender initial digital file; a sender printer configured to: receive the

sender initial digital file; apply a predetermined halftoning process to the sender initial digital file to generate a first digital halftone file comprising a first plurality of discrete digital values; perform a predetermined mathematical process on the first plurality of discrete digital values to thereby generate a sender authentication key; and display the sender authentication key to a sender; (col. 8:56-9:44; 10:61-64)

n. a receiver computer configured to receive the electronic document file from the sender as a receiver initial digital file; a receiver printer configured to: receive the receiver initial digital file; apply the predetermined halftoning process to the receiver initial digital file to generate a second digital halftone file comprising a second plurality of discrete digital values; perform the predetermined mathematical process on the second plurality of discrete digital values to thereby generate a receiver authentication key. (col. 9:63-10:48, especially 10:36-41; the inverse of the signature is a compressed version of N'; embedded matrix M is transformed to compressed version of half tone N, a match authenticates the document)

25. Tresser does not disclose displaying a copy of the authentication key to a user via one of a printer or a user display. Brundage discloses a system for authenticating identification documents using a watermark, wherein an authenticator displays the watermark information to a user to allow an inspector or officer to visually compare the watermark information against information printed on the document. Paragraph 62. It would be obvious to one of ordinary skill in the art at the time the invention was made to

display a copy of the authentication key to a user via one of a printer or a user display. One would be motivated to do so to enable a human to quantify the authenticity of the document as taught by Brundage, *ibid*. The aforementioned cover the limitations of claim 23.

26. Claims 20, 21, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tresser in view of Brundage and further in view of Linsker.

27. As per claims 20 and 21, the rejection of claim 19 under 35 USC 103(a) as being unpatentable over Tresser and Brundage are incorporated herein. Tresser does not disclose the system further comprising a modem configured to receive the initial digital file from a sender and communicate the file, via the processor, to the computer readable memory device; and one of a telephone or a facsimile machine configured to receive a sender authentication key that can be compared to the generated authentication key to authenticate the electronic document file. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital document to create a second digest, wherein a match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the system of Tresser

Art Unit: 2132

to further comprise a modem configured to receive the initial digital file from a sender and communicate the file, via the processor, to the computer readable memory device; and one of a telephone or a facsimile machine configured to receive a sender authentication key that can be compared to the generated authentication key to authenticate the electronic document file. One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 20 and 21.

28. As per claims 24 and 25, the rejection of claim 23 under 35 USC 103(a) as being unpatentable over Tresser and Brundage are incorporated herein. Tresser does not disclose the system further comprising a network connection configurable to allow the sender computer to send the sender initial digital file to the receiver computer; and a sender telephone and a receiver telephone to allow the sender to communicate the sender authentication key to the receiver; or a sender facsimile machine and a receiver facsimile machine to allow the sender to communicate the sender authentication key to the receiver. Linsker discloses using an authentication key to verify the integrity of a fax transmission from a sender to a receiver. The authentication key is based on a digest of a digital document and signature of the digest, which is appended to the document and faxed to the receiver. The receiver recovers the first digest from the signature then performs an operation on the digital document to create a second digest, wherein a

match between the first and second digest shows that the document is authentic. Col. 6:33-8:15. It would be obvious to one of ordinary skill in the art at the time the invention was made for the system of Tresser to further comprise a network connection configurable to allow the sender computer to send the sender initial digital file to the receiver computer; and a sender telephone and a receiver telephone to allow the sender to communicate the sender authentication key to the receiver; or a sender facsimile machine and a receiver facsimile machine to allow the sender to communicate the sender authentication key to the receiver. One would be motivated to do so to ensure the authenticity of documents transmitted via fax using an authentication key derived from halftoning digital information, a process that provides the requisite security, whether or not the document was scanned properly. (Linsker, 1:43-55; Tresser, 3:49-55) The aforementioned cover the limitations of claims 24 and 25.

Conclusion

29. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2132

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Communications Inquiry


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung Kim
AU 2132



GILBERTO BARRON JA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100